Digital cultural heritage in the crossfire of conflict: cyber threats and cybersecurity perspectives

In the digital age, the preservation of digital cultural heritage faces unforeseen vulnerabilities during conflicts. This article dismantles the illusion of invulnerability in digital repositories and digital archives, revealing their susceptibility to warfare through historical examples and contemporary challenges. The Second World War serves as an example of physical assault on cultural heritage, prompting concerns about potential digital cultural genocide. The recent digital attacks on St. Louis Public Library and France's TV5MONDE serve as examples of malicious assaults on digital cultural heritage. Information warfare, nation-state conflicts, ethnic and cultural suppression and other reasons emerge as potential threats to these digital infrastructures and resources. Beyond vulnerabilities, cybersecurity threats and digital inequality pose significant challenges. Conflict zones also face their own infrastructural challenges. Strategies for resilience are reviewed and suggestions for amendments follow, advocating for a holistic approach that integrates digital and tangible preservation methods, responsible technological advancements, community involvement and international collaboration. The article concludes by emphasizing that a nuanced and comprehensive approach to cultural heritage preservation is required during conflicts. Libraries are positioned as stewards of knowledge, advocating for the protection of our shared cultural legacy amidst fragility and times of conflict.

Keywords

cultural genocide; cybersecurity; digital vulnerability; warfare; advocacy; ethical preservation

CHRISTINA DINH NGUYEN

Cataloguer
University of Toronto Mississauga Library
Canada

Introduction

In the modern age, where information is increasingly digitized, the preservation of cultural heritage – whether it be reading material or not – has found refuge in the realm of digital technology. Libraries and archives, once vulnerable to the physical ravages of war, have sought solace in the promise of virtual sanctuaries. As the digital landscape evolves, the concept of secure digital archives and digital repositories becomes paramount in the ethical and secure management of cultural heritage materials.

Let us first examine how digital archives and digital repositories intersect and differ in their operational goals.

Secure archives, distinguished by their robust security measures and adherence to ethical standards, play a crucial role in safeguarding the integrity, authenticity and confidentiality of archival materials – that is, mainly primary resources that would benefit from long-term retention. Some material types that may be digitized are historical records, manuscripts, photographs and audio recordings. These archives contain highly curated collections with contents of a thematic or organizational structure and, like their physical archive counterparts, they adhere to established archival principles for appraisal, acquisition, arrangement, description, preservation and access. Consider, for example, managing both ethical standards and technological infrastructure guidelines, which ensures the ethical security of archived information; digital archivists often consider data protection and privacy regulations (GDPR in the European Union and HIPAA

'Libraries and archives … have sought solace in the promise of virtual sanctuaries'

in the United States are some good examples) as well as technological infrastructures to enable access to the data in such a secure way. Encryption protocols and access controls can help. For example, digital archives containing indigenous knowledge or artifacts will often require these protocols and controls. The Mukurtu content management system (CMS) is a way to do this – it allows indigenous communities to manage, share and exchange their digital heritage in a sustainable, ethical manner that meets their needs. It hosts projects like the Native Health Database and the Plateau Peoples' Web Portal. Mukurtu (and the institutions that work with Mukurtu (CMS) takes into consideration that digital information is inherently political, and that much of the information it manages has direct historical, social and ethical implications for populations that have suffered, and are still suffering, at the hands of oppressors who misrepresent their data and the social contexts around their data. The access and use of data on the platform, and protection from malicious actors who wish to erase history, therefore, is a central theme.

'Secure archives … play a crucial role in safeguarding the integrity, authenticity and confidentiality of archival materials'

While similar to digital archives, digital repositories instead serve as online platforms for storing, managing and providing access to digital resources that may not be highly curated, including scholarly articles, raw research datasets and multimedia content. Even catalogue records, with rich metadata, are often deposited in digital repositories as information useful to researchers (see the fields of bibliographic studies and information retrieval). In the context of ethical and secure librarianship, digital repositories must prioritize the preservation and accessibility of digital assets while addressing security concerns. This involves implementing measures to protect against cybersecurity threats, ensuring data integrity and authenticity and promoting ethical practices such as respecting intellectual property rights and user privacy. Both digital archives and repositories may use on-premises servers or cloud storage services; in many cases it may even be both. Metadata management is regularly performed, digitization processes are in place to create high-quality digital representation of physical objects and file formats are carefully chosen. Backup and redundancy measures are put in to ensure data durability and availability.

In the November 2023 edition of *Insights*, Alice Prochaska described libraries (and other cultural institutions) as being 'all too often the targets of partisan attack by those who seek to bring human inheritance to ruin, or simply to abuse and misuse it'.[1] As an extension of Prochaska's observations, this article explores the often-overlooked fragility of digital preservation during times of conflict, and presents physical preservation challenges as a foil. While digital archives and repositories appear to offer invulnerability, historical examples and contemporary challenges reveal the potential weaknesses.

'this article explores the often-overlooked fragility of digital preservation during times of conflict'

The illusion of invulnerability

The advent of digital technology heralded a new era for cultural heritage preservation. Libraries and archives, recognizing the potential of digitization, invested heavily in creating virtual replicas of their physical treasures and created extensive records to describe those records. Many collections ostensibly saved knowledge that was about to be lost or made cultural information more accessible to marginalized populations. Some interesting examples of digital collections include the University of Toronto Mississauga Library (UTML)'s 'Rafael Platero Paz Papers',[2] and the University of Toronto Fisher Library's 'Canadian Pamphlets and Broadsides' digital collection.[3] Consider also the aforementioned Mukurtu platform,[4] protecting the most vulnerable of collections in a respectful manner. The allure of the digital realm lies in its perceived invulnerability transcending physical boundaries and promising the eternal safeguarding of knowledge. Yet the recent attacks on the British Library, Toronto Public Library,[5] Museum of Fine Arts Boston and the Rubin Museum of Art's digital systems underscore the fragility of digital repositories and archives, and their susceptibility to malicious actors – whether those actors are out for ransom, or worse: ideological washing. Despite the existing security measures being in

place, these attacks compromise access to valuable cultural heritage materials, disrupting research activities and highlighting the urgent need for more robust and consistent cybersecurity protocols in storage efforts.

'recent attacks … underscore the fragility of digital repositories and archives, and their susceptibility to malicious actors'

Part of the issue is the 'invisibility' of the security infrastructures. We often assume that information held online is somehow always there, somewhere in 'the cloud', in neutral, non-partisan contexts. We do not always recognize that information is currency which can be attacked, let alone that it requires secure storage in physical servers on (usually) domestic soil. The concept of invisible infrastructure and the illusion of invulnerability is rooted in the sophisticated layers of security and redundancy measures that underpin digital archives and repositories. Beneath the surface lies a complex network of technologies and protocols designed to safeguard data integrity, privacy and availability. This infrastructure includes elements such as encryption algorithms, access controls, authentication mechanisms, network monitoring tools and backup systems. While these components may not be immediately apparent to users, they play a crucial role in protecting the repository or archive from various forms of attack.

As an example, consider the robust and redundant storage systems such as LOCKSS (Lots of Copies Keep Stuff Safe) and CLOCKSS (Controlled LOCKSS). LOCKSS operates on the principle of distributed (decentralized) preservation, creating multiple copies of digital assets distributed across geographically diverse locations (hence the 'redundant' aspect of storage, minimizing the risk of permanent data loss). Participating institutions each maintain their copy of the content, collectively forming a resilient network of preservation nodes. While LOCKSS primarily focuses on preserving content redundantly, participating institutions themselves are responsible for implementing access controls, encryption algorithms, authentication mechanisms and network monitoring tools at their respective nodes to ensure the security and integrity of the stored data. In contrast, CLOCKSS serves as a centralized service, collecting content from participating libraries and archives and storing it in secure, redundant storage facilities for long periods of time (dark archive). Similarly, CLOCKSS relies on the participating institutions to implement security measures, albeit in a centralized manner. Both systems employ regular validation and synchronization processes to maintain the integrity and authenticity of archived materials. This redundancy not only enhances data resilience against cyber-attacks and technical failures but also mitigates the risks associated with natural disasters or geopolitical conflicts. Thus, LOCKSS and CLOCKSS play crucial roles in reinforcing the security and reliability of digital cultural heritage repositories, countering the illusion of invulnerability by implementing tangible measures to ensure the preservation and accessibility of valuable knowledge for future generations, see Table 1.

Feature	CLOCKSS	LOCKSS
Preservation model	Centralized	Decentralized
Content storage	Stored in secure, redundant central facilities	Copies distributed across participating institutions; the onus is on the institutions to provide security
Access controls	Implemented by participating institutions	Implemented by participating institutions
Encryption	Dependent on participating institutions' setup	Dependent on participating institutions' setup
Authentication	Dependent on participating institutions' setup	Dependent on participating institutions' setup
Network monitoring	Dependent on participating institutions' setup	Dependent on participating institutions' setup
Validation process	Regular validation and synchronization	Regular validation and synchronization
Resilience	Resistant to centralized failure	Resistant to node failure

Table 1. A chart comparing the features of CLOCKSS and LOCKSS

The illusion of invulnerability also arises from the perception that digital repositories (and sometimes archives), with their invisible infrastructure and advanced security measures, are impervious to conflict, abuse and partisan attacks. This perception may be reinforced by high-profile breaches or incidents where repositories successfully withstood attempted intrusions. However, it is essential to recognize that no system is entirely immune to threats, and maintaining the illusion of invulnerability can lead to complacency and neglect of security practices.

Furthermore, the illusion of invulnerability often rests on the assumption that digital artifacts can be easily replicated or restored. However, the loss of unique manuscripts, historical documents and artifacts defies the simplistic notion that the digital realm ensures an effortless recovery of cultural heritage and related research. The intangible aspects, such as the historical context and cultural significance imbued in each artifact, cannot be replicated digitally.

'maintaining the illusion of invulnerability can lead to complacency and neglect of security practices'

Consider also, while security measures are integral to the protection of digital repositories, assuming invulnerability based solely on technological fortifications is a dangerous oversimplification. The illusion comes from a failure to consider the complex nature of conflicts, where both physical and digital spaces become battlegrounds. Therefore, a balanced approach involves acknowledging the limitations of security measures and incorporating resilience into the very fabric of digital preservation strategies. This resilience encompasses not only technological safeguards but also measures to mitigate the impact of conflicts in the communities that these repositories and archives serve.

Historical precedents: creeping towards destruction beyond the physical realm?

The Second World War stands as an overwhelming example of the physical assault on cultural heritage, where libraries and archives both faced systematic destruction by Axis and Allied forces alike. *The Rape of Europa*: *the Fate of Europe's Treasures*,[6] as chronicled by Lynn Nicholas, exposed the extent of looting, bombing and deliberate destruction on museums, libraries and archives across Europe. The cultural heritage lost during this period, estimated at over 100 million books and millions of archival collections, remains an indelible scar on human history. The Nazis, driven by a sinister motivation to obliterate the cultural memory of nations, targeted libraries and archives as part of their ideological warfare. Jewish families faced the theft, confiscation and forced sales of their property, leading to irreversible losses. The restoration efforts that followed the war, while commendable, could never fully resurrect the extent of what was lost.

Cultural genocide will not exist in the physical realm alone. Information professionals must update their mental images of the metaphorical destruction of a library through fire. There is a legitimate concern that adversaries may leverage digital vulnerabilities to perpetrate a form of cultural genocide. By targeting digital repositories, malevolent actors could erase entire cultures, ethnicities and identities from the global collective memory, leaving future generations with an incomplete narrative of human history. Consider these possibilities, many of which are extensions of challenges we face(d) with physical destruction:

'There is a legitimate concern that adversaries may leverage digital vulnerabilities to perpetrate a form of cultural genocide'

- Information warfare: states involved in information warfare may target digital repositories to manipulate historical narratives and public perception. By erasing or distorting digital records, these actors seek to shape global opinions and control the narrative surrounding key events.
- Nation-state conflicts: in the context of geopolitical rivalries, nation-states engaged in conflicts may employ cyber capabilities to disrupt and destroy the digital repositories of their adversaries. This could extend beyond military targets to include cultural heritage sites, erasing the digital footprint of an entire nation.

- Ethnic and cultural suppression: states engaged in ethnic or cultural conflicts may intentionally erase digital records to suppress the history and heritage of targeted groups. This erasure could be a tool for promoting homogeneity and asserting dominance over marginalized populations.

- Authoritarian regimes: authoritarian governments, seeking to maintain control and suppress dissent, could target digital repositories to erase historical records that challenge their narrative. By manipulating collective memories, these regimes aim to solidify their hold on power and control the prevailing historical discourse.

- Religious extremism: religious extremist groups may seek to erase digital representations of cultural practices or historical events that contradict their interpretation of faith. This form of cultural cleansing serves their goal of imposing a singular world-view.

In Richard Ovenden's *Burning the Books: A History of the Deliberate Destruction of Knowledge*, he provided two more insightful cases of online repositories of knowledge (not specifically research data repositories, but similar) being altered for malicious ulterior motives:

> The knowledge held in Wikipedia is subject to attack. Public relations companies have, for instance, been paid to edit or remove material which their clients find uncomfortable. A popular beverage, the beer Stella Artois used to be nicknamed the "wife-beater". This is a verifiable fact backed up by sources and included in the Wikipedia article about Stella Artois. Such a nickname is no longer tolerated in Western society and at one point this was deleted. The account that did this turned out to belong to the PR company Portland Communications. Members of the Wikipedia community restored the deleted references.
>
> Politicians have deleted unwelcome references in Wikipedia to the so-called "expenses scandal" (a series of revelations made by the *Daily Telegraph* and other newspapers relating to illegal expense claims made by Members of Parliament). By analysing the IP addresses of computers that made changes to the biographies of those MPs, the journalist Ben Riley-Smith uncovered the fact that the references, although verifiably in the public domain, were deleted by staff within the Palace of Westminster.[7]

Cybersecurity threats and digital inequality

The point we have hopefully been driving home is that digital repositories and archives, besides facing physical destruction, are also vulnerable to cybersecurity threats during times of conflict. The chaos and instability inherent in physical and information warfare creates opportunities for malicious actors to exploit digital weaknesses. The intentional targeting of digital heritage has become a real and pressing concern. Hacking, data breaches and cyber-attacks on digital libraries can result in the manipulation, theft or destruction of cultural artifacts. Consider, for example, a 'peacetime' case. The recent cyber-attack on the British Library, orchestrated by the hacking group Rhysida, exemplifies the intersection of cybersecurity threats and digital inequality, echoing themes explored in this article. Despite the British Library's status as a prominent cultural institution with significant resources, the attack exposed vulnerabilities in its security infrastructure, leading to widespread disruptions in access to scholarly resources and educational materials. In 2017, the St Louis Public Library[8] system was infected by ransomware and in 2016, France's TV5[9] channel was attacked similarly. The cyber-attacking group claimed association with ISIS. They successfully breached the TV5's systems, disrupting its broadcasting operations and hijacking its social media accounts. While the immediate impact was on TV5MONDE's ability to broadcast and disseminate content, the incident also raised concerns about the

'digital repositories and archives … are also vulnerable to cybersecurity threats during times of conflict'

security of digital cultural heritage. TV5MONDE serves as a platform for promoting French language and culture globally, showcasing a wide range of cultural programming, including documentaries, films and educational content.

Obviously, the cyber-attack on the British Library not only disrupted its physical operations but also severely impacted its digital resources, rendering them inaccessible to users.[10] The library's extensive online catalogue, which serves as a gateway to millions of digital assets including scholarly articles, digitized manuscripts, historical documents and archival materials, became unavailable due to the attack. Additionally, online services such as exhibition ticket sales, reader registrations and access to digital collections were disrupted, further limiting the ability of researchers, students and the public to engage with the library's vast repository of knowledge. This incident underscores the critical importance of robust cybersecurity measures to safeguard digital resources, which play a vital role in facilitating global access to information and advancing scholarly inquiry. This incident highlights the challenges faced by even well-established institutions in safeguarding against sophisticated cyber threats. Moreover, it underscores the disproportionate impact of such attacks on underserved communities, which may rely heavily on digital resources provided by libraries and archives for academic research and learning opportunities. Thus, addressing cybersecurity threats must go hand in hand with efforts to bridge digital divides, ensuring equitable access to information and safeguarding the integrity of digital repositories for all users.

How much worse would it be in an out-and-out conflict? In the midst of such conflict, where political and ideological motivations often drive attacks, the intentional targeting of digital repositories further compounds the challenges of preservation. Consider these types of attacks and weaknesses in repositories, for example:

- Malware and ransomware attacks on digital repositories: malicious software, including ransomware, poses a significant threat to digital repositories. Attackers may encrypt or compromise digital records, demanding a ransom for their release. In the absence of proper cybersecurity measures, institutions risk losing access to critical cultural resources.

- Advanced Persistent Threats (APTs): APTs, often state-sponsored, target digital repositories with sophisticated and prolonged cyber campaigns. These attacks aim to steal sensitive information, disrupt operations, or, in some cases, erase digital records for strategic purposes. Consider this: state actors may have various motivations for targeting public infrastructure digitally, including institutions like the British Library. These motivations could range from espionage and intelligence-gathering to disrupting the operations of adversaries or exerting influence on geopolitical matters. However, it is essential to note that attributing cyber-attacks to specific state actors can be complex and may require thorough investigation by cybersecurity experts and intelligence agencies. While there may be suspicions or indications of state involvement based on the nature and objectives of the attack, definitive evidence linking a cyber-attack to a particular state actor is not always readily available or easily discernible.

- Loss of authenticity and integrity: cybersecurity breaches can compromise the authenticity and integrity of digital cultural heritage. Manipulation of records, insertion of false information or unauthorized alterations undermine the trustworthiness of digital repositories.

- Accessibility and availability issues: successful cyber-attacks may lead to service disruptions, making digital cultural heritage temporarily or permanently inaccessible. This impedes researchers, educators and the public from benefiting from the wealth of information stored in these repositories, particularly changing tides in conflicts classed as 'information wars'.

- Obsolete technology and inadequate infrastructure: outdated technology and insufficient infrastructure create vulnerabilities in digital preservation efforts. Institutions relying on obsolete systems may struggle to fend off cyber threats, making them susceptible to attacks targeting their digital repositories.

Beyond physical and cybersecurity vulnerabilities, there are often limited resources to plan for agile responses to cyber-attacks. Limited funding in digital cultural heritage institutions often translates to insufficient investment in cybersecurity measures, leaving them more vulnerable to cyber-attacks. With constrained resources, these institutions may struggle to implement robust security protocols, conduct regular cybersecurity assessments or deploy advanced threat detection technologies. Consequently, they become attractive targets for malicious actors seeking to exploit their vulnerabilities for financial gain or to disrupt cultural and historical resources. Moreover, the lack of adequate funding may hinder staff training and awareness programs, increasing the likelihood of human error leading to security breaches. To mitigate these risks, it is imperative for policymakers and stakeholders to recognize the importance of investing in cybersecurity for digital cultural heritage institutions, ensuring the protection and preservation of invaluable cultural assets for future generations.

'there are often limited resources to plan for agile responses to cyber-attacks'

Plus, another barrier exists in conflict zones, which often grapple with technological inequality, hindering the effective implementation of digital preservation strategies. Regions facing warfare may lack the necessary technological infrastructures, including reliable electricity and internet connectivity, impeding widespread digitization initiatives. Todd Hutchins has identified internet access as 'humanity's most important resource in war[time]'.[11] The periodization of digital preservation may inadvertently exacerbate existing inequalities, as tangible artifacts and manuscripts hold cultural significance. So, in conflict zones, where communities face serious displacement and disrupted access to education, relying solely on digital formats can contribute to the erasure of cultural identities.

Consider also the fragility of long-term digital storage, with evolving risks that even the most stable of places face. Digital preservation assumes the longevity of storage media and file formats. However, the rapid evolution of technology and the obsolescence of storage formats pose inherent risks to the long-term viability of digital archives. In conflict zones, where the immediate focus is on survival and reconstruction, maintaining and updating digital infrastructure may become secondary priorities, leading to potential data loss over time.

But what to do about it all?

A practical approach to resilience

Ensuring resilience in digital archives and repositories involves implementing a multifaceted approach that addresses various aspects of cybersecurity and data management. Firstly, adherence to established standards such as the Trustworthy Repositories Audit & Certification (TRAC)[12] framework is essential. TRAC provides comprehensive guidelines for assessing the trustworthiness of digital repositories, covering areas like organizational infrastructure, digital object management and security measures. By aligning with TRAC standards, institutions can enhance their resilience against cyber threats by implementing robust policies and procedures for data integrity, authenticity verification and access control.

Moreover, continuous monitoring and proactive risk management are crucial components of resilience strategies for digital archives and repositories. This includes regular security audits, vulnerability assessments and threat intelligence-gathering to identify and address potential weaknesses in the system. Implementing advanced security technologies such as intrusion detection systems, encryption mechanisms and access monitoring tools can bolster defenses against cyber-attacks. Additionally, investing in staff training and awareness programs to foster a culture of cybersecurity vigilance within the organization is paramount. By integrating these resilience strategies into their operational framework, digital archives and repositories can better safeguard their collections and ensure the long-term preservation of cultural heritage in the digital age.

'continuous monitoring and proactive risk management are crucial components of resilience strategies for digital archives and repositories'

Strategies for resilience: a holistic approach

Addressing the vulnerabilities of digital preservation during conflict requires a comprehensive and holistic approach. This involves integrating digital and tangible preservation methods, leveraging technological advancements responsibly and acknowledging the social and cultural dimensions of heritage.

Here are some approaches that complement each other.

Integration of digital and tangible preservation methods

One key aspect of a holistic approach is the integration of both digital and tangible preservation methods. While digital repositories offer unprecedented accessibility and storage efficiency, tangible methods such as physical backups and printed records provide a resilient fallback. Institutions should adopt a dual strategy that combines the benefits of digital and tangible preservation, ensuring redundancy and safeguarding against digital threats.

Responsible technological advancements

Embracing technological advancements is crucial for enhancing digital preservation capabilities. However, it is equally important to do so responsibly. Implementing cutting-edge cybersecurity measures, staying abreast of evolving threats and adopting encryption technologies are essential components of this approach. Responsible technological integration ensures that digital repositories remain at the forefront of preservation without compromising security, and indeed may promote just computing.

Acknowledging social and cultural dimensions of heritage

Digital preservation extends beyond the technical realm; it is deeply intertwined with social and cultural dimensions. Recognizing the importance of heritage in the collective identity of communities is fundamental. This involves engaging with local communities, understanding their perspectives and incorporating their insights into preservation strategies. By acknowledging the cultural significance of digital heritage, institutions can build stronger connections with the communities they serve.

Community involvement and education

A resilient digital preservation strategy involves active community involvement and education. Empowering communities to understand the value of their digital heritage and equipping them with the knowledge to contribute to its preservation fosters a sense of ownership. Educational initiatives can include workshops, awareness campaigns and collaborative projects that bridge the gap between preservation institutions and the communities they serve.

Open standards and interoperability

Establishing open standards and ensuring interoperability among digital preservation systems are vital components of a holistic approach. Open standards facilitate collaboration and information exchange, allowing institutions to share best practices and collectively address emerging challenges. Interoperability ensures that diverse digital repositories can work seamlessly together, creating a networked and resilient infrastructure.

Ethical considerations in preservation

Ethical considerations play a pivotal role in digital preservation during conflicts. Institutions must navigate issues such as data ownership, privacy and the responsible use of emerging technologies. Establishing ethical guidelines and frameworks for decision-making ensures that preservation efforts align with societal values and contribute positively to the broader cultural landscape. The aforementioned Mukurtu platform, as a digital place, recognizes the unique perspectives these communities have in managing and sharing their digital

cultural heritage, at a time when indigenous culture is in an information war – knowledge is appropriated, stolen and attacked. Mukurtu takes ethics into play with access controls, flexible metadata, etc. for the datasets it stewards.

International collaboration and information sharing

Collaboration on an international scale is essential for building a resilient global network of digital preservation. Sharing information, expertise and resources among institutions and countries creates a united front against threats. International collaboration also fosters a collective responsibility for the protection of cultural heritage, transcending geopolitical boundaries.

International co-operation: a collective responsibility

These endeavors are not solely the responsibility of one political party, of one government or even of one nation. There must be a collective responsibility. Actions can include:

Shared threats, shared solutions

The threats faced by digital repositories during conflicts are not confined by national borders. Cybersecurity threats, geopolitical instability and natural disasters can impact institutions worldwide. Recognizing these shared threats prompts a collective responsibility to develop and implement shared solutions. Collaborative efforts can lead to the establishment of global standards, best practices and co-ordinated responses to emerging challenges.

Information exchange and expertise sharing

Digital preservation institutions and professionals worldwide possess diverse expertise and experiences. International co-operation facilitates the exchange of information and sharing of best practices, enabling institutions to learn from each other's successes and failures. This collaborative learning environment enhances the overall resilience of digital repositories by leveraging a wealth of global knowledge.

Resource allocation and support

Many institutions, especially those in conflict-prone regions, may face resource constraints. International co-operation allows for the equitable distribution of resources, including funding, technology and expertise. By pooling resources on a global scale, countries and institutions with more significant capabilities can support those facing challenges, fostering a sense of solidarity in the preservation community.

Crisis response and rapid assistance

During conflicts, digital repositories may face sudden and severe threats. International co-operation enables the development of rapid response mechanisms for crisis situations. Establishing protocols for swift assistance, including the sharing of backup resources and expertise, ensures that affected institutions can quickly recover and mitigate potential losses.

Policy harmonization

The formulation of consistent and harmonized policies is crucial for effective digital preservation. International co-operation facilitates the development of policies that align with global standards, addressing legal, ethical and technical aspects of preservation. Harmonized policies create a framework that institutions worldwide can adhere to, promoting a unified and robust approach to digital heritage protection.

Cultural diplomacy and cross-cultural understanding

Cultural heritage is a testament to the diversity of human experiences. International co-operation in digital preservation fosters cultural diplomacy by celebrating and respecting this diversity. Collaborative projects that involve cross-cultural understanding and exchange contribute to a more interconnected and tolerant global society.

Capacity building and training programs

Building the capacity of institutions and professionals in conflict-prone regions is a vital aspect of international co-operation. Training programs, workshops and mentorship initiatives supported by the global preservation community empower individuals and organizations to strengthen their resilience against digital threats. Consider practices like the sharing of digitization hardware or server space.

Advocacy for cultural heritage protection

International co-operation amplifies advocacy efforts for cultural heritage protection. By uniting voices on a global stage, institutions can influence international policies and agreements that prioritize the preservation of digital heritage during conflicts. This is where librarians can use their talents well. Joint advocacy underscores the significance of cultural preservation in the broader context of global peace and understanding. In conclusion, international co-operation is not merely an option but a necessity in the realm of digital preservation during conflicts. It embodies a collective responsibility to protect our shared cultural heritage, transcending geographical, political and cultural boundaries. By working together, nations and institutions can fortify the resilience of digital repositories, ensuring that the stories, memories and identities embedded in our digital heritage endure for generations to come.

Conclusion

In the nexus of conflict and culture, the fragility of digital cultural heritage infrastructures becomes apparent. Acknowledging the vulnerabilities of digital repositories and archives during times of conflict is not a dismissal of their importance, but a call for a nuanced and comprehensive approach to cultural heritage preservation. The lessons of history echo through the digital age, reminding us that the destruction of cultural heritage transcends physical artifacts to encompass the intangible threads that binds societies together. As we navigate the challenges of preserving cultural heritage during conflicts, we must strive for a harmonious integration of digital and tangible preservation methods, uphold ethical considerations and foster international co-operation. In this endeavor, libraries stand as beacons of knowledge, advocating for the protection of our shared cultural legacy and ensuring that, even in the crossfire of conflict, the richness of human history endures for generations to come.

'libraries stand as beacons of knowledge, advocating for the protection of our shared cultural legacy and ensuring that … the richness of human history endures for generations to come'

Abbreviations and Acronyms
A list of the abbreviations and acronyms used in this and other *Insights* articles can be accessed here – click on the URL below and then select the 'full list of industry A&As' link: http://www.uksg.org/publications#aa.

Competing interests
The author has declared no competing interests.

References

1. Alice Prochaska, "Librarianship in Times of Conflict," *Insights* 36, no. 1 (November 2023): 22, DOI: https://doi.org/10.1629/uksg.639 (accessed 11 March 2024).
2. "About the Rafael Platero Paz Papers," Archives & Special Collections, University of Toronto Mississauga Library, https://collections.utm.utoronto.ca/collections/rafael-platero-paz (accessed 11 March 2024).
3. "Canadian Pamphlets and Broadsides," Thomas Fisher Rare Book Library, https://fishercollections.library.utoronto.ca/islandora/object/broadsides%3Aroot (accessed 11 March 2024).
4. "Our Archives, Our Stories," Mukurtu, https://mukurtu.org/project/our-archives-our-stories/ (accessed 11 March 2024).
5. Maan Alhmidi, "Toronto Public Library gradually recovering from hack, more services back in February," The Canadian Press, *CBC News*, https://www.cbc.ca/news/canada/toronto/toronto-library-cyberattack-1.7089419 (accessed 11 March 2024).
6. Lynn H. Nicholas, *The Rape of Europa: The Fate of Europe's Treasures in the Third Reich and the Second World War*, (Vintage Books USA, 1995).
7. Richard Ovenden, *Burning the Books: A History of the Deliberate Destruction of Knowledge,* (Cambridge, Massachusetts: First Harvard University Press paperback edition, The Belknap Press of Harvard University Press, 2022).
8. Graham Cluley, "Ransomware Attack Hits St Louis Public Library," welivesecurity, 2017, https://www.welivesecurity.com/2017/01/20/ransomware-attack-hits-st-louis-public-library/ (accessed 11 March 2024).

9. Gordon Corera, "How France's TV5 Was Almost Destroyed by 'Russian Hackers'," *BBC News*, 2016, https://www.bbc.com/news/technology-37590375 (accessed 11 March 2024).
10. Gareth Harris, "As British Library Faces Fallout of Cyber Attack – What can art bodies do to combat ransomware threats?," *The Art Newspaper*, December 22, 2023, https://www.theartnewspaper.com/2023/12/22/as-british-library-faces-fallout-of-cyber-attackwhat-can-arts-bodies-do-to-fight-off-wave-of-ransomware-threats (accessed 11 March 2024).
11. Todd Emerson Hutchins, "Safeguarding Civilian Internet Access during Armed Conflict: Protecting Humanity's Most Important Resource in War," *Science and Technology Law Review* 22, no. 1 (2021): 127–80, DOI: https://doi.org/10.52214/stlr.v22i1.8056 (accessed 11 March 2024).
12. "TRAC Metrics," CRL, retrieved 24 February, 2024, https://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/trac (accessed 11 March 2024).

Corresponding author:
Christina Dinh Nguyen
Cataloguer
University of Toronto Mississauga Library
Canada
E-mail: christinadinh.nguyen@utoronto.ca
ORCID ID: https://orcid.org/0000-0003-0938-9836

To cite this article:
Nguyen CD, "Digital cultural heritage in the crossfire of conflict: cyber threats and cybersecurity perspectives," *Insights*, 2024, 37: 7, 1–11; DOI: https://doi.org/10.1629/uksg.647

Submitted on 17 November 2023 Accepted on 27 February 2024 Published on 07 May 2024

Published by UKSG in association with Ubiquity Press.